UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/924,712	08/08/2001	Jeffrey John Jancula	13575.340	3981

21878 7590 10/06/2005

KENNEDY COVINGTON LOBDELL & HICKMAN, LLP
214 N. TRYON STREET
HEARST TOWER, 47TH FLOOR
CHARLOTTE, NC 28202

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/924,712	JANCULA, JEFFREY JOHN	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-87,89 and 90* is/are pending in the application.

4a) Of the above claim(s) *88* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-26,28-33,36-42,44-54,56-59,61-69,71-79,81-87,89 and 90* is/are rejected.

7)☒ Claim(s) *2, 24, 27, 34-35, 43, 55, 60, 70 and 80* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated July 5, 2005 with the amendment to claim 24 and the cancellation of claim 88.

Claims 1-87 and 89-90 are pending.

Response to Arguments

2. Applicant's arguments, filed July 5, 2005, with respect to the rejection(s) of claim(s) 1-87 and 89-90 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Asay et al. (5,903,882), Schneier (Applied Cryptography) and Stallings (Cryptography and Network security).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3-7, 13-17, 22-23, 25-26, 28-33, 36-38, 41-42, 44-48, 53-54, 56-59, 61-63, 68-69, 71-73, 78-79 and 81-84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asay et al. (5,903,882).

a) As to claims 1, 41 and 78, Asay discloses a method and system for supporting reliance on digital signature certificates and managing the risk of such certificates in an electronic transaction system comprising establishing a relationship among the parties (i.e. collective relationship among certification authority, subscriber, relying party and reliance server, Fig. 3); creating a document initiated by one of the parties (Fig. 3, element 112, including primary certificate which specifying the reliance limit); adding verifying information to the document about each of the parties to the document in order to validate the document (col.16, line 21- col. 17, line 4; Fig. 5); adding an expiration time to the document in order to validate the document (col. 13, lines 61-63; col. 12, line 29-col. 14, lines 15); at least one of the parties presenting the document to at least one other of the parties prior to communication of the confidential information therebetween (col. 18, lines 16-54) and the other of the parties permitting the communication of the confident information (i.e. granting supplemental assurance) therebetween only if the document is valid and the expiration time has not passed (col. 18, line 56- col. 19, line 46). The expiration time is first disclosed in the primary certificate (col. 13, lines 61-63), and in the publish certificate message where the reliance server can issue supplemental assurance based on the primary certificate's period (col. 12, lines 45-48) or any specified time period (col. 12, lines 49-51).

Asay does not disclose adding verifying information pertaining to the third party to the document, however Asay discloses the verifying information pertaining to each of the first and second being added to the document.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement adding verifying information pertaining to the third party to the electronic ticket as Asay discloses in the step of adding verifying information pertaining to the first and second to the electronic ticket so as to securely acknowledge and confirmed transmitted data.

b) As to claims 3 and 44, Asay discloses at least a portion of the document is encrypted (col. 17, lines 32-34).

c) As to claims 4, 14, 28, 36, 45, 56, 61, 71 and 81, Asay discloses at least a portion of the document is encrypted (col. 17, lines 32-34) and public key encryption (col. 1, lines 33-52). However he does not disclose at least a portion of the document is symmetrically encrypted.

The examiner takes official notice that the use of symmetric encryption is very well-known in the data encryption art.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of symmetric encryption in the system of Asay so as to provide another effective means of encryption.

d) As to claims 5, 15, 29, 37, 46, 57, 62, 72 and 82, Asay discloses at least a portion of the document is encrypted (see addressed claim 3), however he does not explicitly disclose at least a portion of the document is asymmetrically encrypted, however he discloses public key encryption (col. 1, lines 33-52). It anticipates that public key encryption can be implemented as claimed.

e) As to claims 6, 16, 22, 47 and 83, Asay discloses the document includes a digital signature of first party (Fig. 3, element 114), however he does not disclose document includes digital signature of each of the parties.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement including digital signature of each of the parties in the document as Asay discloses so as to securely acknowledge and confirmed transmitted data.

f) As to claims 7 and 17, 38, 48, 63, 73 and 84, Asay discloses the encrypted information is capable of decryption using an encryption key (col. 17, lines 35-36).

g) As to claims 13, 25, 53, 58 and 68, Asay discloses a method and system for supporting reliance on digital signature certificates and managing the risk of such certificates in an electronic transaction system comprising establishing an electronic communication relationship among all the parties (i.e. collective relationship among certification authority, subscriber, relying party and reliance server, Fig. 3); creating an electronic ticket initiated by a first of the parties (Fig. 3, element 112, including primary certificate which specifying the reliance limit); adding security information pertaining to the first party to the electronic ticket (Fig. 3, element 114) and then sending the electronic ticket to a second of the parties (Fig. 3, element 108); adding security information pertaining to the second party to the electronic ticket (Fig. 5) and then sending the electronic ticket to a third of the parties (Fig. 3, element 104); validating the electronic ticket by verifying the security information pertaining to the at least three parties; at least one of the parties presenting the electronic ticket to another of the

parties prior to communicating confidential information therebetween (col. 18, lines 16-54) and the other of the parties permitting the communication of confident information (i.e. granting supplemental assurance) therebetween only after the electronic ticket is validated.

Asay does not disclose adding security information pertaining to the third party to the electronic ticket, however Asay discloses the security information pertaining to each of the first and second being added to the electronic ticket. It would have been obvious to one of ordinary skill in the art at the time of the invention to implement adding security information pertaining to the third party to the electronic ticket as Asay discloses in the step of adding security information pertaining to the first and second to the electronic ticket so as to securely acknowledge and confirmed transmitted data.

h) As to claims 23, 26, 32, 42, 54, 59, 69 and 79, this limitation is addressed in claim 1.

i) As to claim 30, Asay discloses a method and system for supporting reliance on digital signature certificates and managing the risk of such certificates in an electronic transaction system comprising requiring the security document to be presented to the first party by one of the second and third parties prior to permitting the communication of confidential information (col. 18, lines 16-54); permitting the communication of confidential information (i.e. granting supplemental assurance) of the second party with the third party only after verifying that the security document is valid (col. 18, line 56 to col. 19, line 46).

Asay does not disclose adding encrypted security information pertaining to the first party to a security document, however Asay discloses the security information pertaining to each of the second and third being added to the security document (Fig. 3, element 114; Fig. 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement adding encrypted security information pertaining to the first party to the security document as Asay discloses in the step of adding security information pertaining to the second and third to the electronic ticket so as to securely acknowledge and confirmed transmitted data.

j) As to claims 31 and 33, Asay discloses the invention relates to electronic transactions which automatically performs services as requested by the relying party (Abstract), it anticipates the security document is an electronic document, the encrypted security information being added electronically, the confidential information being communicated electronically and the expiration time is added electronically .

5. Claims 10-11, 20-21, 51-52, 66-67, 76-77, 87 and 89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asay et al. (5,903,882) in view of Schneier (Applied Cryptography).

Asay does not disclose the private key is a multiple use key or a one-time use key.

Schneier discloses the lifetime of a key wherein some key can be used one time and other key could be used multiple times over a period of time (page 183-184).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of determining the permitted lifetime of a key as Schneier teaches in the system of Asay so as to reduce number of attacks.

6. Claims 8-9, 12, 18-19, 39-40, 49-50, 64-65, 74-75, 85-86 and 90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asay et al. (5,903,882) in view of Stallings (Cryptography and Network Security).

a) As to claims 8-9, 18-19, 39-40, 49-50, 64-65, 74-75 and 85-86, Asay discloses public key encryption (col. 1, lines 33-52). However he does not disclose the encryption key is a public key or a private key.

Stallings discloses encryption key is a public key or a private key (page 165-166).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of public key or private key as encryption key in the system of Asay as Stalling teaches so as to securely protect communicated data.

b) As to claims 12 and 90, Stallings discloses the encrypted information is encrypted with a public key and capable of decryption using a private key (Fig. 6.1 on page 166).

Allowable Subject Matter

7. Claims 2, 24, 27, 34-35, 43, 55, 60, 70 and 80 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in

independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
9/30/05

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER